Safeguards for social networking:

Keep your guard up on sites like Facebook, LinkedIn and Twitter. Scammers are exploiting the trust we have of our connections on these sites to gain access to your accounts and commit fraud.

Fake Notification E-mails

Look out for fake emails that look like they came from Facebook. These typically include links to phony pages that attempt to steal your login information or prompt you to download malware. Never click on links is suspicious emails. Log-in to a site directly.

Suspicious posts and Messages

Wall posts or messages that appear to come from a friend asking you to click on a link to check out a new photo or video that doesn't actually exist. The link is typically for a phony login page or a site that will put a virus on your computer to steal your passwords.

Money Transfer Scams

Messages that appear to come from friends or others claiming to be stranded and asking for money. These messages are typically from scammers. Ask them a question that only they would be able to answer. Or contact the person by phone to verify the situation, even if they say not to call them.

General Online Safety Rules

- **Be wary of strangers** – The internet makes it easy for people to misrepresent their identities and motives. If you interact with strangers, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical** – People may post false or misleading information about various topics, including their own. Try to verify the authenticity of any information before taking any action.

- **Evaluate your settings** – Use privacy settings. The default settings for some sites may allow anyone to see your profile. Even private information could be exposed, so don't post anything that you wouldn't want the public to see.
- **Use strong passwords** – Protect your account with passwords that cannot be easily guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

Security Information For Social Networking Sites

www.facebook.com/security

www.twitip.com/twitter-security-dos-and-donts

www.linkedin.com/secure/settings

Actions to Avoid

1. **Don't click on a message that seems weird.** If it seems unusual for a friend to write on your Wall and post a link, that friend may have gotten phished.
2. **Don't enter your password through a link.** Just because a page on the Internet looks like Facebook, it doesn't mean it is. It is best to go to the Facebook log-in page though your browser.
3. **Don't use the same password on Facebook that you use in other places on the web.** If you do this, phishers or hackers who gain access to one of your accounts will easily be able to access your others as well, including your bank.
4. **Don't share your password with anyone.** Social sites will never ask for your password through any form of communication.
5. **Don't click on links or open attachments in suspicious e-mails.** Fake e-mails can be very convincing, and hackers can spoof the "From:" address so the e-mail looks like it's from a social site. If the e-mail looks weird, don't trust it, and delete it from your inbox.
6. **Don't send money anywhere** unless you have verified the story of someone who says they are your friend or relative.

7. **Don’t provide your cell phone number to verify the results of a Facebook game or survey without reading the terms and conditions.** It may result in recurring charges on your cell phone bill.

More resource Information:

www.us-cert.gov or www.fbi.gov